

REMARKS

Claims 1-4 are pending.

Claims 1-4 are rejected.

Claim 1 is amended for clarity and to change the "only" language of the claim to support the embodiment of the invention supported in paragraph 0038 of the specification. That is, the specification recites that the second device has the second symmetric key. In addition, the Applicants are attempting to amend Claim 1 to affirmative cite method steps.

No new matter was added in view of these amendments.

ARGUMENTS

Rejection of Claims 1-4 under 35 U.S.C. 103

The Examiner rejected Claims 1-4 under 35 U.S.C. 103 as being unpatentable over Menezes et al. "Handbook of Applied Cryptography, PASSAGE" Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FL., CRC Press, US 1997, pages 497-533 (hereafter 'Menezes'), in view of US Patent Publication No. 2005/0025901 to Patel et al. (hereafter 'Patel'). Applicants disagree with this ground of rejection.

The Examiner claims that claimed element of "the first symmetric key encrypted using a second symmetric network key known by the device of the second type" is found in the prior art. Applicants disagree with this assertion. Specifically, unlike the aspect that $E_{K_{AT}}(K)$, this is not the case, as B neither has K_{AT} or $E_{K_{AT}}(K)$. While it is true that device A after reception of the message from T has $E_{K_{AT}}(K)$, but A decrypts this to obtain k. There is no reason whatever for A to transmit the encrypted key to B or for B to be in possession of it, unlike what is stated by the Examiner.

That is, B does receive $E_{K_{BT}}(k)$, but this aspect of the prior art is the encryption of the first symmetric key using a third key that is known to a device of a third type (not

second type unlike the present claim). Hence A does not know this key, as is as required by the claim.

In addition, the claimed step of "said encrypted first symmetric key" being transmitted to a device of a second type is not performed in the prior art in that "B" does not have the encrypted first symmetric key. Therefore, B cannot send such a key, unlike what the Examiner claims is taught in the cited prior art.

For the reasons given above, the Applicants assert that Claim 1 is patentable over the cited art of record. In addition, Claims 2-4 are patentable over the cited prior for the reasons given above. The Examiner is encouraged to speak with the Applicants' representative to discuss any issues that can help this application proceed to allowance.

Respectfully submitted,

Alain Durand et al.

By: /Joel M. Fogelson/
Joel M. Fogelson
Attorney for Appellants
Reg. No. 43,613
Phone (818) 480-5318

Patent Operations
Thomson Licensing LLC
P. O. Box 5312
Princeton, New Jersey 08540

May 5, 2011